



SMB 服务器支持

ONTAP 9

NetApp
April 24, 2024

目录

- SMB 服务器支持 1
 - SMB 服务器支持概述 1
 - 支持的 SMB 版本和功能 1
 - 不支持的 Windows 功能 3
 - 在 SVM 上配置 NIS 或 LDAP 名称服务 4
 - ONTAP 名称服务交换机配置的工作原理 6

SMB 服务器支持

SMB 服务器支持概述

您可以在 Storage Virtual Machine （SVM）上启用和配置 SMB 服务器，以使 SMB 客户端能够访问集群上的文件。

- 集群中的每个数据 SVM 只能绑定到一个 Active Directory 域。
- 数据 SVM 不需要绑定到同一个域。
- 多个 SVM 可以绑定到同一个域。

在创建 SMB 服务器之前，您必须配置用于提供数据的 SVM 和 LIF。如果您的数据网络不平整，则可能还需要配置 IP 空间，广播域和子网。网络管理指南 _ 包含详细信息。

相关信息

["网络管理"](#)

[修改 SMB 服务器](#)

["系统管理"](#)

支持的 SMB 版本和功能

服务器消息块（SMB）是 Microsoft Windows 客户端和服务端使用的一种远程文件共享协议。在 ONTAP 9 中，支持所有 SMB 版本；但是，默认 SMB 1.0 支持取决于您的 ONTAP 版本。您应验证 ONTAP SMB 服务器是否支持环境中所需的客户端和功能。

有关 ONTAP 支持的 SMB 客户端和域控制器的最新信息，请参见 *Interoperability Matrix Tool*。

默认情况下，ONTAP 9 SMB 服务器会启用 SMB 2.0 及更高版本，并且可以根据需要启用或禁用这些版本。下表显示了 SMB 1.0 支持和默认配置。

SMB 1.0 功能：	在以下 ONTAP 9 版本中：			
	9.0	9.1.	9.2.	9.3及更高版本
默认情况下处于启用状态	是的。	是的。	是的。	否
可以启用或禁用	否	是 * 需要 9.1 P8 或更高版本。	是的。	是的。



与域控制器的 SMB 1.0 和 2.0 连接的默认设置也取决于 ONTAP 版本。有关详细信息、请参见 `vserver cifs security modify` 手册页。对于现有 CIFS 服务器运行 SMB 1.0 的环境，您应尽快迁移到更高的 SMB 版本，以便为增强安全性和合规性做好准备。有关详细信息，请联系您的 NetApp 代表。

下表显示了每个 SMB 版本支持的 SMB 功能。默认情况下，某些 SMB 功能处于启用状态，某些功能需要额外配置。

* 此功能: *	* 需要启用: *	对于以下 SMB 版本: *, ONTAP 9 支持 *				
		1.0	2.0	2.1.	3.0	3.1.1
旧版 SMB 1.0 功能		X	X	X	X	X
耐用手柄			X	X	X	X
复合操作			X	X	X	X
异步操作			X	X	X	X
读取和写入缓冲 冲区大小增加			X	X	X	X
提高可扩展性			X	X	X	X
SMB 签名	X	X	X	X	X	X
备用数据流 (ADS) 文件格式	X	X	X	X	X	X
大型 MTU (从 ONTAP 9.7 开始，默认情况下处于启用状态)	X			X	X	X
租用机会锁				X	X	X
持续可用的共享	X				X	X
持久句柄					X	X
见证					X	X

* 此功能： *	* 需要启用： *	对于以下 SMB 版本： *， ONTAP 9 支持 *				
SMB 加密： AES-128-CCM	X				X	X
横向扩展（ CA 共享需要 ）					X	X
透明故障转移					X	X
SMB 多通道（ 从 ONTAP 9.4 开始）	X				X	X
预身份验证完 整性						X
集群客户端故 障转移 v.2 （ CCFv2）						X
SMB 加密： AES-128- GCM （从 ONTAP 9.1 开 始）	X					X

相关信息

[使用 SMB 签名增强网络安全性](#)

[设置 SMB 服务器的最低身份验证安全级别](#)

[在 SMB 服务器上配置通过 SMB 传输数据所需的 SMB 加密](#)

["NetApp 技术报告 4543：《SMB 协议最佳实践》"](#)

["NetApp 互操作性"](#)

不支持的 Windows 功能

在网络中使用 CIFS 之前，您需要了解 ONTAP 不支持的某些 Windows 功能。

ONTAP 不支持以下 Windows 功能：

- 加密文件系统（EFS）
- 在更改日志中记录 NT 文件系统（NTFS）事件

- Microsoft 文件复制服务（FRS）
- Microsoft Windows 索引服务
- 通过分层存储管理（HSM）实现远程存储
- 从 Windows 客户端管理配额
- Windows 配额语义
- LMHOSTS 文件
- NTFS 原生压缩

在 SVM 上配置 NIS 或 LDAP 名称服务

通过 SMB 访问，即使访问 NTFS 安全模式卷中的数据，也始终会执行用户到 UNIX 用户的映射。如果将 Windows 用户映射到信息存储在 NIS 或 LDAP 目录存储中的相应 UNIX 用户，或者使用 LDAP 进行名称映射，则应在 SMB 设置期间配置这些名称服务。

开始之前

您必须已自定义名称服务数据库配置，以匹配名称服务基础架构。

关于此任务

SVM 使用名称服务 ns-switch 数据库确定查找给定名称服务数据库源的顺序。ns-switch 源可以是 "files"，"nis" 或 "ldap" 的任意组合。对于组数据库，ONTAP 会尝试从所有已配置的源获取组成员资格，然后使用整合的组成员资格信息进行访问检查。如果在获取 UNIX 组信息时其中一个源不可用，则 ONTAP 无法获取完整的 UNIX 凭据，后续访问检查可能会失败。因此，您必须始终检查 ns-switch 设置中是否为组数据库配置了所有 ns-switch 源。

默认情况下，SMB 服务器会将所有 Windows 用户映射到本地存储的默认 UNIX 用户 passwd 数据库。如果要使用默认配置，可选择配置 NIS 或 LDAP UNIX 用户和组名称服务或 LDAP 用户映射以进行 SMB 访问。

步骤

1. 如果 UNIX 用户、组和网络组信息由 NIS 名称服务管理，请配置 NIS 名称服务：

a. 使用确定名称服务的当前顺序 `vserver services name-service ns-switch show` 命令：

在此示例中，三个数据库 (group, passwd, 和 netgroup) nis 作为名称服务源、仅使用 files 作为源。

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	files
vs1	passwd	true	files
vs1	netgroup	true	files
vs1	namemap	true	files

您必须添加 nis 源到 group 和 passwd 数据库、并可选择添加到 netgroup 数据库。

- b. 使用根据需要调整名称服务ns-switch数据库的顺序 `vserver services name-service ns-switch modify` 命令：

为了获得最佳性能，您不应向名称服务数据库添加名称服务，除非您计划在 SVM 上配置该名称服务。

如果修改多个名称服务数据库的配置，则必须为要修改的每个名称服务数据库单独运行此命令。

在此示例中、nis 和 files 配置为的源 group 和 passwd 数据库、按此顺序。其余名称服务数据库保持不变。

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

- c. 使用验证名称服务的顺序是否正确 `vserver services name-service ns-switch show` 命令：

```
vserver services name-service ns-switch show -vserver vs1
```

Vserver	Database	Enabled	Source Order
-----	-----	-----	-----
vs1	hosts	true	dns, files
vs1	group	true	nis, files
vs1	passwd	true	nis, files
vs1	netgroup	true	files
vs1	namemap	true	files

- d. 创建NIS名称服务配置：+ `vserver services name-service nis-domain create -vserver vserver_name -domain NIS_domain_name -servers NIS_server_IPaddress,... -active true+`

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60 -active true
```



从ONTAP 9.2开始、此字段为 `-nis-servers` 替换字段 `-servers`。此新字段可以使用NIS服务器的主机名或IP地址。

- e. 验证NIS名称服务是否已正确配置且处于活动状态：`vserver services name-service nis-domain show vserver vserver_name`

```
vserver services name-service nis-domain show vserver vs1
```

Vserver	Domain	Active	Server
vs1	example.com	true	10.0.0.60

2. 如果 UNIX 用户，组和网络组信息或名称映射由 LDAP 名称服务管理，请使用位于的信息配置 LDAP 名称服务 ["NFS 管理"](#)。

ONTAP 名称服务交换机配置的工作原理

ONTAP会将名称服务配置信息存储在一个表中、该表相当于 `/etc/nsswitch.conf` 文件。您必须了解该表的功能以及 ONTAP 如何使用它，以便可以根据您的环境对其进行适当配置。

ONTAP 名称服务切换表可确定 ONTAP 为检索特定类型的名称服务信息而查询的名称服务源。ONTAP 会为每个 SVM 维护一个单独的名称服务切换表。

数据库类型

该表为以下每种数据库类型存储一个单独的名称服务列表：

数据库类型	定义名称服务源 ...	有效源为 ...
主机	将主机名转换为 IP 地址	文件， DNS
组	查找用户组信息	文件， nis ， ldap
密码	查找用户信息	文件， nis ， ldap
网络组	正在查找网络组信息	文件， nis ， ldap
命名映射	正在映射用户名	文件， LDAP

源类型

源用于指定用于检索相应信息的名称服务源。

指定源类型 ...	查找信息的位置	由命令系列管理 ...
文件	本地源文件	<pre>vserver services name- service unix-user vserver services name-service unix-group vserver services name- service netgroup vserver services name- service dns hosts</pre>
NIS	在 SVM 的 NIS 域配置中指定的外部 NIS 服务器	<pre>vserver services name- service nis-domain</pre>
ldap	在 SVM 的 LDAP 客户端配置中指定的外部 LDAP 服务器	<pre>vserver services name- service ldap</pre>
DNS	在 SVM 的 DNS 配置中指定的外部 DNS 服务器	<pre>vserver services name- service dns</pre>

即使您计划使用NIS或LDAP进行数据访问和SVM管理身份验证、也仍应包括 `files` 并将本地用户配置为在NIS或LDAP身份验证失败时的回退。

用于访问外部源的协议

要访问外部源的服务器， ONTAP 使用以下协议：

外部名称服务源	用于访问的协议
NIS	UDP
DNS	UDP
LDAP	TCP

示例

以下示例显示了SVM的名称服务开关配置 `svm_1`：

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
```

Vserver	Database	Source Order
-----	-----	-----
svm_1	hosts	files, dns
svm_1	group	files
svm_1	passwd	files
svm_1	netgroup	nis, files

要查找用户或组信息，ONTAP 仅会查找本地源文件。如果查询未返回任何结果，则查找将失败。

要查找网络组信息，ONTAP 首先会查找外部 NIS 服务器。如果查询未返回任何结果，则接下来会检查本地网络组文件。

SVM SVM_1 的表中没有用于名称映射的名称服务条目。因此，默认情况下，ONTAP 仅会查找本地源文件。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。